ARTIN–HASSE-TYPE SERIES AND ROOTS OF UNITY

KEITH CONRAD

1. Introduction

The p-adic exponential function $e^X = \sum_{i\geq 0} X^i/i!$ has disc of convergence

$$D = \{x \in \mathbf{C}_p : |x|_p < (1/p)^{1/(p-1)}\}. \tag{1.1}$$

In this disc the p-adic exponential function is an isometry: $|e^x - e^y|_p = |x-y|_p$ for $x, y \in D$. In particular, e^x is not a root of unity for any $x \in D$ other than $x = 0$: if $(e^x)^n = 1$ for some $n \in \mathbf{Z}^+$ then $0 = |e^{nx} - 1|_p = |e^{nx} - e^0|_p = |nx|_p$, so $nx = 0$ and thus $x = 0$.

In contrast to e^X, we'll see in Section 2 that the Artin–Hasse exponential series

$$\mathrm{AH}(X) := \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \frac{X^{p^3}}{p^3} + \cdots\right) = \exp\left(\sum_{i\geq 0}\frac{X^{p^i}}{p^i}\right) \tag{1.2}$$

converges on the larger disc $\mathfrak{m}_p = \{x \in \mathbf{C}_p : |x|_p < 1\}$ and at well-chosen x in $\mathfrak{m}_p$, $\mathrm{AH}(x)$ runs over the pth-power roots of unity in $\mathbf{C}_p$. This is a p-adic analogue of the complex-analytic representation of roots of unity as $e^{2\pi i a/b}$ for rational a/b, but it is limited to roots of unity in $\mathbf{C}_p$ with p-power order. This property of $\mathrm{AH}(X)$ in p-adic analysis is well known, but a proof is not written down in too many places.

Truncating the exponent in $\mathrm{AH}(X)$ to a polynomial leads to truncated Artin–Hasse series

$$\mathrm{AH}_n(X) = \exp\left(X + \frac{X^p}{p} + \cdots + \frac{X^{p^n}}{p^n}\right)$$

for $n \geq 0$; $\mathrm{AH}_0(X)$ is e^X. For $n \geq 1$, $\mathrm{AH}_n(X)$ converges on a disc between D and $\mathfrak{m}_p$ and has some p^n-th roots of unity as values but not necessarily all of them. We treat $n = 1$ in Section 3 and general n in Section 4. Section 5 has statistics for coefficients of $\mathrm{AH}(X)$.

I thank Sandi Xhumari for his comments and for pointing out Theorem 4.9.

2. Getting pth power roots of unity from $\mathrm{AH}(X)$

The series $\mathrm{AH}(X)$ is the composition of two series with p-adically large coefficients: those of e^X are $1/i!$ and the nonzero coefficients in $\sum_{i\geq 0} X^{p^i}/p^i$ run through reciprocal powers of p. Amazingly, after composing these series to get $\mathrm{AH}(X)$, the coefficients are bounded.

Theorem 2.1. *The coefficients of* $\mathrm{AH}(X)$ *are in* $\mathbf{Z}_p$.

Proof. We will give two proofs. The first is somewhat specific to the series $\mathrm{AH}(X)$, while the second has a wider scope of applicability.

For a first proof we use a representation of $\mathrm{AH}(X)$ as an infinite product that closely resembles an infinite product representation of e^X:

$$e^X = \prod_{k\geq 1}(1-X^k)^{-\mu(k)/k}, \quad \mathrm{AH}(X) = \prod_{\substack{k\geq 1\\ p\nmid k}}(1-X^k)^{-\mu(k)/k}.$$

Each of these formulas can be verified by taking the logarithmic derivative (that is, pass from $f(X)$ to $f'(X)/f(X)$) of both sides and checking the results are equal. Therefore the two sides of the original formulas are equal up to a nonzero scaling factor, and since both sides start with constant term 1 the scaling factor is 1. When $p \nmid k$ the fraction $-\mu(k)/k$ is a p-adic integer (either 0 or a p-adic unit), so $(1-X^k)^{-\mu(k)/k} = \sum_{i\geq 0}\binom{-\mu(k)/k}{i}(-1)^iX^{ik}$ has coefficients in $\mathbf{Z}_p$.[1] Thus $\mathrm{AH}(X) \in 1 + X\mathbf{Z}_p[[X]]$.

For a second proof we use Dwork's lemma, which says a series $f(X)$ in $1+X\mathbf{Q}_p[[X]]$ is in $1+X\mathbf{Z}_p[[X]]$ if and only if $f(X)^p/f(X^p) \in 1+p\mathbf{Z}_p[[X]]$. When $f(X) = \mathrm{AH}(X)$, we have

$$\frac{f(X)^p}{f(X^p)} = \frac{\exp(pX + X^p + X^{p^2}/p + \cdots)}{\exp(X^p + X^{p^2}/p + X^{p^3}/p^2 + \cdots)} = e^{pX} = \sum_{i\geq 0}\frac{p^i}{i!}X^i,$$

and $p^i/i! \in p\mathbf{Z}_p$ for $i \geq 1$ since

$$\mathrm{ord}_p(p^i/i!) = i - \frac{i - s_p(i)}{p-1} = \left(1 - \frac{1}{p-1}\right)i + \frac{s_p(i)}{p-1} \geq \frac{s_p(i)}{p-1} > 0.$$

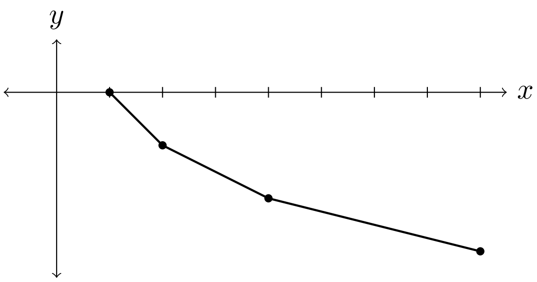
□

We can work out the initial coefficients of $\mathrm{AH}(X)$ explicitly to see that they lie in $\mathbf{Z}_p$. Rewriting $\mathrm{AH}(X)$ as $e^Xe^{X^p/p+X^{p^2}/p^2+\cdots}$, the second factor is a series in X^p whose first two nonzero terms are $1 + X^p/p$, so in $\mathbf{Q}[[X]]$ we have

$$\begin{aligned}\mathrm{AH}(X) &\equiv e^X\left(1+\frac{X^p}{p}\right) \bmod X^{p+1}\\ &\equiv \left(1 + X + \frac{X^2}{2!} + \cdots + \frac{X^p}{p!}\right)\left(1+\frac{X^p}{p}\right) \bmod X^{p+1}\\ &\equiv 1 + X + \frac{1}{2!}X^2 + \cdots + \frac{1}{(p-1)!}X^{p-1} + \frac{1+(p-1)!}{p!}X^p \bmod X^{p+1}.\end{aligned}$$

Thus $\mathrm{AH}(X)$ has ith coefficient $1/i!$ for $0 \leq i \leq p-1$ and $(1+(p-1)!)/p!$ for $i = p$. The coefficients up through X^{p-1} are p-adic units, while the coefficient of X^p is in $\mathbf{Z}_p$ by Wilson's theorem, which says $(p-1)! \equiv -1 \bmod p$.

Since $\mathrm{AH}(X)$ is in $\mathbf{Z}_p[[X]]$, it converges on $\mathfrak{m}_p$. (We'll see at the end of this section that $\mathfrak{m}_p$ is the full disc of convergence.) The series $\sum_{i\geq 0}X^{p^i}/p^i$ also converges on $\mathfrak{m}_p$, and its Newton polygon (see picture for $p = 2$ below) has ith segment connecting $(p^{i-1}, -(i-1))$ to $(p^i, -i)$: its horizontal length is $p^i - p^{i-1} = \varphi(p^i)$ and its slope is $-1/\varphi(p^i)$. Thus each nonzero root of $\sum_{i\geq 0}X^{p^i}/p^i$ in $\mathbf{C}_p$ has valuation $1/\varphi(p^j)$ for some $j \geq 1$ and there are $\varphi(p^j)$ roots in $\mathbf{C}_p$ with valuation $1/\varphi(p^j)$, where roots are counted with multiplicity. Each root is simple since the derivative $\sum_{i\geq 0}X^{p^i-1} = 1 + X^{p-1} + X^{p^2-1} + \cdots$ doesn't vanish on $\mathfrak{m}_p$.



[1] For any $c \in \mathbf{Z}_p$, the binomial coefficient $\binom{c}{i}$ is in $\mathbf{Z}_p$ since $\binom{c}{i}$ is a polynomial in c, hence p-adically continuous in c, and c is a p-adic limit of positive integers c_n. Therefore $\binom{c}{i}$ is a p-adic limit of $\binom{c_n}{i}$, which are all integers, so their limit is in $\mathbf{Z}_p$.

We will show for each root x of $\sum_{i\geq 0} X^{p^i}/p^i$ in $\mathfrak{m}_p$ with $\mathrm{ord}_p(x) = 1/\varphi(p^j)$ that $\mathrm{AH}(x)$ is a root of unity of order p^j. In particular, $\mathrm{AH}(x) \neq 1$. That is a surprise: if $\sum_{i\geq 0} x^{p^i}/p^i = 0$ shouldn't (1.2) imply $\mathrm{AH}(x) = \exp(\sum_{i\geq 0} x^{p^i}/p^i) = \exp(0) = 1$? No! In (1.2) the power series are formal (with X an indeterminate), and to say there is a *numerical* equality

$$\mathrm{AH}(x) = \exp\left(\sum_{i\geq 0} \frac{x^{p^i}}{p^i}\right) \tag{2.1}$$

for some $x \in \mathbf{C}_p$, on the left side we must use the definition of evaluating a power series, which requires writing the series in standard form as $\sum_{k\geq 0} a_k X^k$, not any other expression, *before* substituting a number for the indeterminate in the series. We'll see in Corollary 2.6 that (2.1) holds for x sufficiently close to 0 in $\mathfrak{m}_p$, but not if x gets too far from 0 in $\mathfrak{m}_p$.

Justifying (2.1) for small x in $\mathbf{C}_p$ is a special case of the following situation. Let $f(X) \in \mathbf{C}_p[[X]]$ and $g(X) \in X\mathbf{C}_p[[X]]$, with $h(X) = f(g(X))$ being the formal composition. When $g(x)$, $f(g(x))$, and $h(x)$ all converge at some $x \in \mathbf{C}_p$, $h(x)$ is not automatically equal to $f(g(x))$ even though $h(X) = f(g(X))$ because computing the number $h(x)$ requires substituting x into $h(X)$ when it is written as a power series in standard form, not in the composite form $f(g(X))$. Rewriting $f(g(X))$ as a power series in X to get $h(X)$ doesn't depend on the magnitude of the coefficients of f and g, but when trying to turn $f(g(x))$ into $h(x)$ these are series of numbers and the magnitudes of the coefficients of f and g can interact with the magnitude of x to cause problems if f and g have large coefficients. And the case for us, $f(X) = \exp(X)$ and $g(X) = \sum_{i\geq 0} X^{p^i}/p^i$, has series with large coefficients!

The next theorem gives conditions under which a formal power series identity $h(X) = f(g(X))$ turns into a numerical identity $h(x) = f(g(x))$ at a number x.

Theorem 2.2. *For $f(X) \in \mathbf{C}_p[[X]]$ and $g(X) \in X\mathbf{C}_p[[X]]$, let $h(X) = f(g(X))$ be their composition and $g(X) = \sum_{i\geq 0} c_i X^i$. For $x \in \mathbf{C}_p$ such that $g(x)$ converges and $|c_i x^i|_p < r_f$ for all $i \geq 0$, where r_f is the radius of convergence of $f(X)$, we have $f(g(x))$ converges, $h(x)$ converges, and $f(g(x)) = h(x)$.*

Proof. See [4, Theorem, Section 6.1.5], where the coefficients of the series are in any field K that is a complete extension field of $\mathbf{Q}_p$ in $\mathbf{C}_p$. □

Remark 2.3. A result similar to Theorem 2.2 is [2, Theorem 4.3.3], whose difference is that the hypothesis "$|c_i x^i|_p < r_f$ for all $i \geq 0$" is replaced with "$f(g(x))$ converges and $|c_i x^i|_p \leq |g(x)|_p$ for all $i \geq 0$," so the first conclusion of Theorem 2.2 is shifted to a hypothesis. The inequalities $|c_i x^i|_p \leq |g(x)|_p$ for all i are equivalent to $\max |c_i x^i|_p = |g(x)|_p$ since always $|g(x)|_p \leq \max |c_i x^i|_p$. In practice most p-adic power series $f(X)$ of interest (*e.g.*, $f(X) = e^X$) have an open disc of convergence, in which case $f(g(x))$ converges if and only if $|g(x)|_p < r_f$, so Theorem 2.2 implies [2, Theorem 4.3.3] in this situation. Each of our uses of Theorem 2.2 below can be replaced with [2, Theorem 4.3.3], but it is often much easier to verify the hypothesis of Theorem 2.2 than of [2, Theorem 4.3.3]. A third theorem justifying substitution into a composition of power series is [5, Lemma 41.2].

Theorem 2.4. *If $|x|_p < (1/p)^{1/(p-1)}$ then (2.1) is true.*

Proof. We use Theorem 2.2 with $f(X) = e^X$ and $g(X) = \sum_{i\geq 0} X^{p^i}/p^i$, so $r_f = (1/p)^{1/(p-1)}$. If $|x|_p < (1/p)^{1/(p-1)}$ check $|x^{p^i}/p^i|_p < |x|_p$ for $i \geq 1$, so $|x^{p^i}/p^i|_p < r_f$ for $i \geq 0$. □

If $(1/p)^{1/(p-1)} \leq |x|_p < 1$ then it turns out (2.1) is not true because $\mathrm{AH}(x)$ is outside the range of the exponential series. This will follow from $\mathrm{AH}(X)$ being an isometry on $\mathfrak{m}_p$.

Theorem 2.5. *For x and y in $\mathfrak{m}_p$, $|\operatorname{AH}(x)-\operatorname{AH}(y)|_p = |x-y|_p$. In particular, for $x \in \mathfrak{m}_p$, $|\operatorname{AH}(x)-1|_p = |x|_p$.*

Proof. Pick x and y in $\mathfrak{m}_p$. We can assume $x \neq y$, since the isometry is obvious if $x = y$.

Set $\operatorname{AH}(X) = \sum_{k\geq 0} a_k X^k$, so $a_k \in \mathbf{Z}_p$ and $a_0 = a_1 = 1$. Then

$$\operatorname{AH}(x) - \operatorname{AH}(y) = \left(1 + x + \sum_{k\geq 2} a_k x^k\right) - \left(1 + y + \sum_{k\geq 2} a_k y^k\right) = x - y + \sum_{k\geq 2} a_k(x^k - y^k)$$

and we want to show $|\sum_{k\geq 2} a_k(x^k-y^k)|_p < |x-y|_p$. Since $a_k \in \mathbf{Z}_p$ and $a_k(x^k-y^k) \to 0$,

$$\left|\sum_{k\geq 2} a_k(x^k - y^k)\right|_p \leq \max_{k\geq 2} |a_k(x^k-y^k)|_p \leq \max_{k\geq 2} |x^k - y^k|_p.$$

Let $r = \max(|x|_p, |y|_p)$, so $0 < r < 1$. For $k \geq 2$,

$$|x^k - y^k|_p = |x-y|_p|x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1}|_p \leq |x-y|_p \max_{0\leq i\leq k-1} |x|_p^{k-1-i}|y|_p^i.$$

Each term $|x|_p^{k-1-i}|y|_p^i$ is at most $r^{k-1-i}r^i = r^{k-1} \leq r$. Thus $\max_{k\geq 2}|x^k - y^k|_p \leq |x-y|_p r < |x-y|_p$.

For $x \in \mathfrak{m}_p$ and $y = 0$, $|\operatorname{AH}(x)-1|_p = |\operatorname{AH}(x) - \operatorname{AH}(0)|_p = |x-0|_p = |x|_p$. □

Recall from (1.1) that we write D for the p-adic disc of convergence of e^X.

Corollary 2.6. *For $x \in \mathfrak{m}_p$, (2.1) is true if and only if $x \in D$.*

Proof. Theorem 2.4 tells us that if $x \in D$ then (2.1) holds. Conversely, assume $x \in \mathfrak{m}_p$ and (2.1) holds. Then $\operatorname{AH}(x) = e^y$ where $y = \sum_{i\geq 0} x^{p^i}/p^i$ must lie in D; otherwise the right side of (2.1) makes no sense. Since $\exp(D) = 1 + D$ and $|\operatorname{AH}(x) - 1|_p = |x|_p$ by Theorem 2.5, having $\operatorname{AH}(x) \in \exp(D)$ implies $\operatorname{AH}(x) - 1 \in D$, which implies $x \in D$. □

We have shown the only $x \in \mathfrak{m}_p$ for which (2.1) could possibly be true are $x \in D$, and it is true for such x by Theorem 2.4. What can be said about $\operatorname{AH}(x)$ if $x \in \mathfrak{m}_p$ but $x \notin D$? Between 1 and $(1/p)^{1/(p-1)}$ there is a whole sequence of intermediate powers of $1/p$:

$$\left(\frac{1}{p}\right)^{1/(p-1)} < \left(\frac{1}{p}\right)^{1/(p(p-1))} < \left(\frac{1}{p}\right)^{1/(p^2(p-1))} < \cdots < \left(\frac{1}{p}\right)^{1/(p^j(p-1))} < \cdots < 1.$$

Every x in $\mathfrak{m}_p$ satisfies $|x|_p < (1/p)^{1/(p^j(p-1))}$ for some $j \geq 0$. When this happens for $j = 0$, Theorem 2.4 tells us how to write $\operatorname{AH}(x)$ as an exponential value. When this happens for $j \geq 1$, we can't write $\operatorname{AH}(x)$ as an exponential value if $(1/p)^{1/(p-1)} \leq |x|_p < (1/p)^{1/(p^j(p-1))}$, but it turns out we can write $\operatorname{AH}(x)^{p^j}$ as an exponential.

Theorem 2.7. *Fix an integer $j \geq 1$. In $\mathbf{C}_p$,*

$$|x|_p < \left(\frac{1}{p}\right)^{1/(p^j(p-1))} \Longrightarrow \operatorname{AH}(x)^{p^j} = \exp\left(p^j \sum_{i\geq 0} \frac{x^{p^i}}{p^i}\right).$$

In particular, if $\sum_{i\geq 0} x^{p^i}/p^i = 0$ in $\mathbf{C}_p$ with $|x|_p = (1/p)^{1/\varphi(p^j)}$ then $\operatorname{AH}(x)^{p^j} = 1$.

Proof. We have the formal power series identity

$$\operatorname{AH}(X)^{p^j} = \exp\left(p^j \sum_{i\geq 0} \frac{X^{p^i}}{p^i}\right) \tag{2.2}$$

so it's natural to try justifying substitution of x for X on both sides, which is what we'll do. For the left side, substitution of x for X is valid because it is a finite product of power series (copies of $\mathrm{AH}(X)$) that each converge at x. For the right side we want to use Theorem 2.2 with $f(X) = \exp(X)$, $g(X) = p^j \sum_{i\geq 0} X^{p^i}/p^i$, and x satisfying $|x|_p < (1/p)^{1/(p^j(p-1))}$. We need to show $g(x)$ converges and $|p^j x^{p^i}/p^i|_p < (1/p)^{p-1}$ for all $i \geq 0$.

We know $g(x)$ converges since $|x|_p < 1$. Since

$$|p^j x^{p^i}/p^i|_p \overset{?}{<} \left(\frac{1}{p}\right)^{1/(p-1)} \iff \left(\frac{1}{p}\right)^{j-i} |x|_p^{p^i} \overset{?}{<} \left(\frac{1}{p}\right)^{1/(p-1)}$$
$$\iff |x|_p \overset{?}{<} \left(\frac{1}{p}\right)^{(1/(p-1)-(j-i))/p^i},$$

we want to check that

$$\left(\frac{1}{p}\right)^{1/(p^j(p-1))} \leq \left(\frac{1}{p}\right)^{(1/(p-1)-(j-i))/p^i},$$

and that is equivalent to

$$\frac{1}{p^j(p-1)} \geq \frac{1/(p-1)-(j-i)}{p^i},$$

which is equivalent to

$$j - i + \frac{1}{p^{j-i}(p-1)} \geq \frac{1}{p-1}.$$

Here i and j only show up in $j-i$. Let's show for all $k \in \mathbf{Z}$ that $k + 1/(p^k(p-1)) \geq 1/(p-1)$.

(1) If $k = 0$ we have equality.
(2) If $k \geq 1$ the left side is greater than 1, which is greater than or equal to $1/(p-1)$.
(3) If $k \leq -1$ write $k = -\ell$, so we want to show $-\ell + p^\ell/(p-1) \geq 1/(p-1)$, which is equivalent to $(p^\ell - 1)/(p-1) \geq \ell$. By algebra,

$$\frac{p^\ell - 1}{p-1} = \underbrace{1 + p + \cdots + p^{\ell-1}}_{\ell \text{ terms}} \geq \underbrace{1 + 1 + \cdots + 1}_{\ell \text{ terms}} = \ell.$$

That completes the proof of the main implication for this theorem.

All that remains is to observe for $\sum_{i\geq 0} x^{p^i}/p^i = 0$ and $\mathrm{ord}_p(x) = 1/\varphi(p^j)$ that

$$|x|_p = \left(\frac{1}{p}\right)^{1/\varphi(p^j)} = \left(\frac{1}{p}\right)^{1/(p^{j-1}(p-1))} < \left(\frac{1}{p}\right)^{1/(p^j(p-1))},$$

so $\mathrm{AH}(x)^{p^j} = \exp(p^j(0)) = 1$. □

Corollary 2.8. *If $\sum_{i\geq 0} x^{p^i}/p^i = 0$ for $x \in \mathbf{C}_p$ with $\mathrm{ord}_p(x) = 1/\varphi(p^j)$ for $j \geq 1$, then $\mathrm{AH}(x)$ has order p^j.*

Proof. We present two proofs. Both rely on $\mathrm{AH}(X)$ being an isometry, although the second method makes fuller use of that.

Method 1: Since $\mathrm{AH}(X)$ is an isometry on $\mathfrak{m}_p$ it is injective.

If $\mathrm{AH}(x)$ does not have order p^j then $\mathrm{AH}(x)^{p^{j-1}} = 1$. When $\sum_{i\geq 0} y^{p^i}/p^i = 0$ with $y = 0$ or $\mathrm{ord}_p(y) = 1/\varphi(p^k)$ for some $k \leq j-1$ then $\mathrm{AH}(y)^{p^{j-1}} = 1$, and the number of such (distinct) y is $1 + \sum_{k=0}^{j-1} \varphi(p^k) = p^{j-1}$. That accounts for all solutions to $t^{p^{j-1}} = 1$ in $\mathbf{C}_p$, so $\mathrm{AH}(x) = \mathrm{AH}(y)$ for one of those y, and thus $x = y$, but $\mathrm{ord}_p(x) \neq \mathrm{ord}_p(y)$. Thus $\mathrm{AH}(x)$ has order p^j.

Method 2 To compute the order of $\mathrm{AH}(x)$ as a root of unity we will compute $|\mathrm{AH}(x)-1|_p$. The point is that if ζ is a root of unity in $\mathbf{C}_p$ with order p^r then $|\zeta-1|_p = (1/p)^{1/(p^{r-1}(p-1))}$, so we can read off the order of ζ if we know $|\zeta-1|_p$.

From Theorem 2.5, $|\mathrm{AH}(x)-1|_p = |x|_p = (1/p)^{1/\varphi(p^j)} = (1/p)^{1/(p^{j-1}(p-1))}$, so $\mathrm{AH}(x)$ has order p^j. □

The ideas we have presented can be applied to series built in a similar way to $\mathrm{AH}(X)$.

Theorem 2.9. *Let $c_0, c_1, c_2, \ldots$ be a sequence in $\mathbf{Q}_p$ with $c_0 \in \mathbf{Z}_p^\times$. Define*

$$A(X) = \exp\left(\sum_{i\geq 0} c_i \frac{X^{p^i}}{p^i}\right).$$

(1) *We have $A(X) \in \mathbf{Z}_p[[X]]$ if and only if all c_i are in $\mathbf{Z}_p$ and $c_i \equiv c_{i-1} \bmod p^i$ for all $i \geq 1$. In particular, to have $A(X) \in \mathbf{Z}_p[[X]]$ it is necessary that $c_i \in \mathbf{Z}_p^\times$ for $i \geq 1$ if $c_0 \in \mathbf{Z}_p^\times$.*

(2) *Suppose all c_i are in $\mathbf{Z}_p^\times$ and $A(X) \in \mathbf{Z}_p[[X]]$, so $A(X)$ converges on $\mathfrak{m}_p$. Then*
   (a) *$|A(x) - A(y)|_p = |x-y|_p$ for all x and y in $\mathfrak{m}_p$,*
   (b) *for $j \geq 0, |x|_p < \left(\frac{1}{p}\right)^{1/(p^j(p-1))} \Longrightarrow A(x)^{p^j} = \exp\left(p^j \sum_{i\geq 0} c_i \frac{x^{p^i}}{p^i}\right)$.*
   (c) *for each $j \geq 1$ the series $\sum_{i\geq 0} c_i X^{p^i}/p^i$ has $\varphi(p^j)$ simple zeros in $\mathbf{C}_p$ with valuation $1/\varphi(p^j)$, and at these zeros the value of $A(X)$ is a root of unity of order p^j.*

Proof. Left to the reader. □

Theorem 2.10. *The disc of convergence of $\mathrm{AH}(X)$ in $\mathbf{C}_p$ is $\mathfrak{m}_p$.*

Proof. We already know $\mathrm{AH}(X)$ converges on $\mathfrak{m}_p$. If the disc of convergence were any larger than $\mathfrak{m}_p$ then $\mathrm{AH}(X)$ would converge at 1, which is equivalent to saying the coefficients of $\mathrm{AH}(X)$ tend to 0. We will show that $\mathrm{AH}(X)$ has infinitely many coefficients in $\mathbf{Z}_p^\times$, or equivalently the reduction $\mathrm{AH}(X) \bmod p \in \mathbf{F}_p[[X]]$ is *not* in $\mathbf{F}_p[X]$.

By the definition of $\mathrm{AH}(X)$ in (1.2), $\mathrm{AH}'(X) = \mathrm{AH}(X)\sum_{i\geq 0} X^{p^i-1}$. Thus

$$X\frac{\mathrm{AH}'(X)}{\mathrm{AH}(X)} = \sum_{i\geq 0} X^{p^i}.$$

This last equation (not its derivation) only involves series in $\mathbf{Z}_p[[X]]$, so we can reduce both sides mod p and treat it as an equation in $\mathbf{F}_p[[X]]$. Differentiation and reduction mod p commute, so the above equation is also true in $\mathbf{F}_p[[X]]$ where $\mathrm{AH}(X)$ means $\mathrm{AH}(X) \bmod p$, and $\mathrm{AH}'(X)$ is its derivative. The series $f(X) = \sum_{i\geq 0} X^{p^i} = X + X^p + X^{p^2} + \cdots$ satisfies $f(X)^p = f(X) - X$ in characteristic p, so $f(X) \bmod p$ is a root of $T^p - T + X$. It's left to the reader to show $T^p - T + X$ has no root in $\mathbf{F}_p(X)$, so $X\,\mathrm{AH}'(X)/\mathrm{AH}(X) \bmod p$ is not in $\mathbf{F}_p(X)$. Therefore $\mathrm{AH}(X) \bmod p$ is not in $\mathbf{F}_p(X)$. In particular, $\mathrm{AH}(X) \bmod p \notin \mathbf{F}_p[X]$. □

Since $\mathrm{AH}(X) \in 1 + X\mathbf{Z}_p[[X]]$, also $\mathrm{AH}(X)^{-1} \in 1 + X\mathbf{Z}_p[[X]]$, so $\mathrm{AH}(X)^{-1}$ converges on $\mathfrak{m}_p$. A power series and its inverse might not have the same disc of convergence (try $1-X$ and $1/(1-X)$), but for the Artin–Hasse series and its inverse the two discs are the same.

Corollary 2.11. *The disc of convergence of $\mathrm{AH}(X)^{-1}$ in $\mathbf{C}_p$ is $\mathfrak{m}_p$.*

Proof. The proof of Theorem 2.10 showed $\mathrm{AH}(X) \bmod p \notin \mathbf{F}_p(X)$, so $\mathrm{AH}(X)^{-1} \bmod p \notin \mathbf{F}_p(X)$ as well. Therefore $\mathrm{AH}(X)^{-1} \bmod p \notin \mathbf{F}_p[X]$, so $\mathrm{AH}(X)^{-1}$ has infinitely many coefficients in $\mathbf{Z}_p^\times$ and thus does not converge at 1. □

3. Getting pth roots of unity from $\exp(X + X^p/p)$

Consider the truncated Artin–Hasse series

$$E(X) = e^{X+X^p/p},$$

where we keep only the first two terms from the exponent of $\mathrm{AH}(X)$.[2] Both e^X and $e^{X^p/p}$ have disc of convergence $D = \{x \in \mathbf{C}_p : |x|_p < (1/p)^{1/(p-1)}\}$, but their product $E(X)$ turns out to have a larger disc of convergence that lies between D and $\mathfrak{m}_p$. (Unlike $\mathrm{AH}(X)$, $E(X)$ is not in $\mathbf{Z}_p[[X]]$.) Analogously to what we saw with $\mathrm{AH}(X)$, our goal is to show $E(X)$ has nontrivial pth roots of unity as values at the nonzero roots of its exponent $X + X^p/p$.

To find the disc of convergence of $E(X)$, we first argue without checking details carefully. Write $E(X)$ as the infinite product

$$E(X) = \mathrm{AH}(X) \prod_{j \geq 2} e^{-X^{p^j}/p^j}. \tag{3.1}$$

where each factor has a different disc of convergence in $\mathbf{C}_p$:

- $\mathrm{AH}(X)$ has disc of convergence $\mathfrak{m}_p$.
- $e^{-X^{p^j}/p^j}$ has disc of convergence

$$D_j := \{x \in \mathbf{C}_p : |x|_p < (1/p)^{(j+1/(p-1))/p^j}\} \tag{3.2}$$

(so $D_0 = D_1 = D$). The containments $D_1 \subset D_2 \subset \cdots \subset D_j \subset \cdots \subset \mathfrak{m}_p$ are strict.

In (3.1), each factor $e^{-X^{p^j}/p^j}$ for $j \geq 2$ converges on D_2, as does $\mathrm{AH}(X)$, so $E(X)$ should converge on D_2. Since $\mathrm{AH}(X)$ and $e^{-X^{p^j}/p^j}$ for $j \geq 3$ all converge on D_3, while $e^{-X^{p^2}/p^2}$ only converges on D_2, it is plausible that $E(X)$ converges precisely on D_2.

The description of the discs of convergence of the factors on the right side of (3.1) are correct, but the reasoning behind $E(X)$ converging on D_2 is incorrect. It was based on the attractive idea that if power series $f_j(X)$ all converge on a common disc and their product $f(X) = \prod f_j(X)$ converges as a formal power series, then $f(X)$ also converges on the same disc. However, this need not be true.

Example 3.1. We can factor the geometric series as an infinite product of polynomials:

$$\sum_{i \geq 0} X^i = \prod_{k \geq 0} (1 + X^{2^k})$$

because each exponent i on the left is a unique sum of powers of 2 (binary expansion). Each polynomial $1 + X^{2^k}$ has an infinite radius of convergence, but the geometric series has a finite radius of convergence.

The error in our reasoning for $E(X)$ to converge on D_2 is that formal convergence of an infinite product of formal power series doesn't depend on the exact magnitude of the coefficients while numerical convergence of the same product does.

Despite the mistake, the result is true: $E(X)$ has disc of convergence D_2. To prove this, we will write the infinite product in (3.1) as a single exponential and apply Theorem 2.2.

Theorem 3.2. *The disc of convergence of $E(X)$ is $D_2 = \{x : |x|_p < (1/p)^{(2+1/(p-1))/p^2}\}$.*

[2] As with $\mathrm{AH}(X)$, the series $E(X)$ depends on p but we don't include this dependence in the notation $E(X)$.

Proof. Rewrite (3.1) as

$$E(X) = \mathrm{AH}(X) \exp\left(\sum_{j\geq 2} -\frac{X^{p^j}}{p^j}\right). \tag{3.3}$$

For the exponential factor on the right we want to apply Theorem 2.2 with $f(X) = \exp(X)$, $g(X) = \sum_{j\geq 2} -X^{p^j}/p^j$, and $x \in D_2$. The hypotheses we have to check for Theorem 2.2 are that $g(x)$ converges and

$$x \in D_2 \Longrightarrow \left|-\frac{x^{p^j}}{p^j}\right|_p < \left(\frac{1}{p}\right)^{1/(p-1)} \quad \text{for } j \geq 2. \tag{3.4}$$

Convergence of $g(x)$ is clear since $g(X)$ converges on $\mathfrak{m}_p$. The inequality in (3.4) is the same as $|x|_p < (1/p)^{(j+1/(p-1))/p^j}$, so we want to show

$$|x|_p < \left(\frac{1}{p}\right)^{(2+1/(p-1))/p^2} \Longrightarrow |x|_p < \left(\frac{1}{p}\right)^{(j+1/(p-1))/p^j} \quad \text{for } j \geq 2,$$

which would follow from

$$\left(\frac{1}{p}\right)^{(2+1/(p-1))/p^2} \leq \left(\frac{1}{p}\right)^{(j+1/(p-1))/p^j} \quad \text{for } j \geq 2,$$

and that is the same as

$$\frac{2+1/(p-1)}{p^2} \geq \frac{j+1/(p-1)}{p^j} \text{ for } j \geq 2.$$

The sequence $\{(j+1/(p-1))/p^j\}$ for $j \geq 1$ is strictly decreasing (this is why the discs D_j are strictly increasing), so we have justified using Theorem 2.2: the standard power series for $f(g(X))$ converges on D_2, as does $\mathrm{AH}(X)$, so $E(X) = \mathrm{AH}(X)f(g(X))$ converges on D_2.

To prove $E(X)$ does not converge on a disc larger than D_2, rewrite (3.3) as

$$e^{-X^{p^2}/p^2} = E(X)\,\mathrm{AH}(X)^{-1} \exp\left(\sum_{j\geq 3} X^{p^j}/p^j\right).$$

The exponential factor on the right, as a standard power series, converges on D_3 by Theorem 2.2, similar to how we just used Theorem 2.2 on $\exp(\sum_{j\geq 2} -X^{p^j}/p^j)$. Also $\mathrm{AH}(X)^{-1}$ converges on D_3 (Corollary 2.11), so if $E(X)$ converges on a disc larger than D_2 then so does $e^{-X^{p^2}/p^2}$, which is false. □

Theorem 3.3. *If $x \in D$ then*

$$E(x) = e^{x+x^p/p}. \tag{3.5}$$

If $x \in D_2$ then

$$E(x)^p = e^{p(x+x^p/p)}. \tag{3.6}$$

In particular, if $x + x^p/p = 0$ in $\mathbf{C}_p$ then $E(x)^p = 1$.

Proof. If $x \in D$ then we obtain (3.5) by applying Theorem 2.2 with $f(X) = \exp(X)$ and $g(X) = X + X^p/p$ at $X = x$: $g(x)$ converges and $|x^p/p|_p < |x|_p < (1/p)^{1/(p-1)} = r_f$.

To prove (3.6) when $x \in D_2$, set $h(X) = E(X)^p$, so $h(X) = \exp(p(X + X^p/p))$ as formal power series. Since $E(X)$ converges on D_2, we have $h(x) = E(x)^p$ since $E(X)^p$ is a finite product of power series that converge at x. To prove $h(x) = \exp(p(x + x^p/p))$ too, we want to apply Theorem 2.2 with $f(X) = \exp(X)$ and $g(X) = p(X + X^p/p) = pX + X^p$ at $X = x$: $g(x)$ converges, and for $x \in D_2$ the reader can check $|px|_p < r_f$ and $|x^p|_p < r_f$.

If $x + x^p/p = 0$ then $x = 0$ or $|x|_p = (1/p)^{1/(p-1)}$, so $x \in D_2$ and we can use (3.6). □

We want to sharpen the end of Theorem 3.3: if $x + x^p/p = 0$ and $x \neq 0$ then $E(x)$ is not just a pth root of unity, but is a nontrivial pth root of unity. This will follow from $E(X)$ being an isometry on its disc of convergence, which is analogous to e^X being an isometry on its disc of convergence. To prove $E(X)$ is an isometry on D_2 we will go back to (3.1) and figure out the size of the power series coefficients of the infinite product (over $j \geq 2$) on the right side. We will use p-adic valuations rather than p-adic absolute values.

Lemma 3.4. *Let $u_j \in \mathbf{Z}_p^\times$ for $j \geq 2$. Writing*

$$\prod_{j\geq 2} e^{u_j X^{p^j}/p^j} = \sum_{k\geq 0} c_k X^k, \tag{3.7}$$

we have $c_k = 0$ if $p^2 \nmid k$, and if $p^2 \mid k$ then

$$\operatorname{ord}_p(c_k) = -\frac{k}{p^2}\left(2 + \frac{1}{p-1}\right) + \frac{s_p(k)}{p-1}, \tag{3.8}$$

where $s_p(k)$ is the sum of the base p digits of k.

We will use Lemma 3.4 only with $u_j = \pm 1$.

Proof. The left side of (3.7) involves X in powers of X^{p^2}, so $c_k = 0$ if $p^2 \nmid k$.

If $p^2 \mid k$, the lower bound $\operatorname{ord}_p(c_k) \geq -(k/p^2)(2+1/(p-1))$ is proved in [3, pp. 321–322]. By running through the argument from [3] more carefully, we will get the exact formula for $\operatorname{ord}_p(c_k)$ in (3.8).

Set $e^{u_j X^{p^j}/p^j} = \sum_{m\geq 0} d_{j,m} X^m$, so

$$d_{j,m} = \begin{cases} 0, & \text{if } p^j \nmid m, \\ u_j^t/(p^{jt}t!), & \text{if } m = p^j t,\ t \in \mathbf{N}. \end{cases}$$

Since $\operatorname{ord}_p(n!) = (n - s_p(n))/(p-1)$ and $\operatorname{ord}_p(u_j) = 0$,

$$p^j \mid m \Longrightarrow \operatorname{ord}_p(d_{j,m}) = -\frac{m}{p^j}\left(j + \frac{1}{p-1}\right) + \frac{s_p(m/p^j)}{p-1} = -\frac{m}{p^j}\left(j + \frac{1}{p-1}\right) + \frac{s_p(m)}{p-1}. \tag{3.9}$$

In (3.7) we have $c_0 = 1$ and for $k \geq 1$ with $p^2 \mid k$,

$$c_k = \sum_{\substack{r\geq 1 \\ m_1,\ldots,m_r\geq 1 \\ m_1+\cdots+m_r=k \\ 2\leq j_1<\cdots<j_r \\ p^{j_1}\mid m_1,\ldots,p^{j_r}\mid m_r}} d_{j_1,m_1}\cdots d_{j_r,m_r}. \tag{3.10}$$

For example, $c_{p^2} = u_2/p^2$. The sum in (3.10) has finitely many terms.

One term in the sum is $d_{2,k}$, which is the contribution from the coefficient of X^k in $\exp(u_2 X^{p^2}/p^2)$, and by (3.9) $\operatorname{ord}_p(d_{2,k}) = -(k/p^2)(2 + \frac{1}{p-1}) + s_p(k)/(p-1)$. We will show every other term in the sum has larger ord_p-value, so

$$\operatorname{ord}_p(c_k) = \operatorname{ord}_p(d_{2,k}) = -\frac{k}{p^2}\left(2 + \frac{1}{p-1}\right) + \frac{s_p(k)}{p-1}$$

if $p^2 \mid k$, including when $k = 0$.

Each term in (3.10) besides $d_{2,k}$ has some $j_i > 2$. If $j > 2$ and $m \geq 1$, then

$$\frac{m}{p^j}\left(j + \frac{1}{p-1}\right) < \frac{m}{p^2}\left(2 + \frac{1}{p-1}\right),$$

so any term in (3.10) besides $d_{2,k}$ has

$$\begin{aligned}\operatorname{ord}_p(d_{j_1,m_1}\cdots d_{j_r,m_r}) &= \sum_{i=1}^{r}\left(-\frac{m_i}{p^{j_i}}\left(j_i+\frac{1}{p-1}\right)+\frac{s_p(m_i)}{p-1}\right)\\ &> \sum_{i=1}^{r}-\frac{m_i}{p^2}\left(2+\frac{1}{p-1}\right)+\frac{s_p(m_1)+\cdots+s_p(m_r)}{p-1}\\ &= -\frac{k}{p^2}\left(2+\frac{1}{p-1}\right)+\frac{s_p(m_1)+\cdots+s_p(m_r)}{p-1}.\end{aligned}$$

Since

$$s_p(m_1)+\cdots+s_p(m_r)-s_p(m_1+\cdots+m_r)=(p-1)\operatorname{ord}_p\left(\frac{(m_1+\cdots+m_r)!}{m_1!\cdots m_r!}\right)\geq 0,$$

and $m_1+\cdots+m_r=k$, we have

$$\operatorname{ord}_p(d_{j_1,m_1}\cdots d_{j_r,m_r})>-\frac{k}{p^2}\left(2+\frac{1}{p-1}\right)+\frac{s_p(k)}{p-1}=\operatorname{ord}_p(d_{2,k}).$$

□

Remark 3.5. Obtaining the strict inequality in the last line is how our argument differs from [3, pp. 321–322]. We used the exact formula for $\operatorname{ord}_p(d_{j,m})$ in (3.9), while [3, p. 321] uses the lower bound on $\operatorname{ord}_p(d_{j,m})$ coming from replacing $s_p(m)/(p-1)$ in (3.9) with 0.

A good way to think about what we proved in this lemma is that the p-adic valuations of the power series coefficients of $\prod_{j\geq 2}e^{u_jX^{p^j}/p^j}$ are controlled by the coefficients of the first factor $e^{u_2X^{p^2}/p^2}$: they are equal in all degrees.

In the proof of Lemma 3.4 we used $u_2\in\mathbf{Z}_p^\times$ but only needed u_j for $j>2$ to be in $\mathbf{Z}_p$, not $\mathbf{Z}_p^\times$, so the lemma is true somewhat more generally than that way it was stated.

Theorem 3.6. *Setting $E(X)=\sum_{k\geq 0}a_kX^k$, we have the upper bound*

$$|a_k|_p\leq p^{(k/p^2)(2+1/(p-1))-1/(p-1)}$$

for $k\geq (p+1)/2$ and not for $k<(p+1)/2$.

Proof. We will check this separately for $k\geq p^2$ and for $k\leq p^2-1$.

Write $E(X)=\operatorname{AH}(X)\prod_{j\geq 2}e^{-X^{p^j}/p^j}=\operatorname{AH}(X)\sum_{i\geq 0}c_iX^i$, so $\operatorname{ord}_p(c_i)$ is given by Lemma 3.4. Since the coefficients of $\operatorname{AH}(X)$ are in $\mathbf{Z}_p$, for $k\geq p^2$ we have

$$\begin{aligned}|a_k|_p &\leq \max_{\substack{0\leq i\leq k\\ p^2\mid i}}|c_i|_p\\ &= \max_{\substack{0\leq i\leq k\\ p^2\mid i}}\left(\frac{1}{p}\right)^{-(i/p^2)(2+1/(p-1))+s_p(i)/(p-1)} \qquad \text{by (3.8)}\\ &= \max_{\substack{0\leq i\leq k\\ p^2\mid i}}p^{(i/p^2)(2+1/(p-1))-s_p(i)/(p-1)}.\end{aligned}$$

In the maximum, the $i=0$ term is 1 and the $i=p^2$ term is $p^{2+1/(p-1)-1/(p-1)}=p^2>1$, so we can ignore $i=0$. Then, since $s_p(i)\geq 1$ for $i\geq 1$, we have for $k\geq p^2$ that

$$|a_k|_p\leq \max_{\substack{1\leq i\leq k\\ p^2\mid i}}p^{(i/p^2)(2+1/(p-1))-1/(p-1)}\leq p^{(k/p^2)(2+1/(p-1))-1/(p-1)}.$$

For $k \leq p^2 - 1$, we have $|a_k|_p \leq 1$ since $E(X)$ and $\mathrm{AH}(X)$ have the same coefficients up to degree $p^2 - 1$. Therefore the upper bound on $|a_k|_p$ in the theorem holds if the exponent $(k/p^2)(2 + 1/(p-1)) - 1/(p-1)$ is nonnegative, which is equivalent to $k \geq p^2/(2p-1)$. Since $\frac{p^2}{2p-1} < \frac{p+1}{2}$, we have $k > p^2/(2p-1)$ when $k \geq (p+1)/2$, so the upper bound on $|a_k|_p$ in the theorem holds for $(p+1)/2 \leq k \leq p^2 - 1$. What if $k < (p+1)/2$? In that case $k < p$, so $a_k = 1/k!$ (the coefficients of $E(X)$ and e^X agree through degree $p-1$) and thus $|a_k|_p = 1$. Therefore the upper bound on $|a_k|_p$ in the theorem is false since for such k the exponent on p in the bound is negative. □

Theorem 3.7. *For all x and y in D_2, $|E(x) - E(y)|_p = |x - y|_p$.*

Proof. We can take $x \neq y$. Writing $E(X) = \sum_{k \geq 0} a_k X^k$, easily $a_0 = a_1 = 1$, so

$$E(x) - E(y) = x - y + \sum_{k \geq 2} a_k(x^k - y^k).$$

To show $|E(x) - E(y)|_p = |x - y|_p$ we will show $|a_k(x^k - y^k)|_p < |x - y|_p$ for all $k \geq 2$. Since $x \neq y$ this inequality is equivalent to $|a_k(x^k - y^k)/(x - y)|_p < 1$, which is the same as

$$|a_k(x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1})|_p < 1. \tag{3.11}$$

Recall $D_2 = \{x \in \mathbf{C}_p : |x|_p < R\}$ for $R = (1/p)^{(2+1/(p-1))/p^2}$. Since x and y are in D_2, each $x^{k-1-i}y^i$ for $0 \leq i \leq k-1$ has absolute value less than $R^{k-1} = (1/p)^{(k-1)(2+1/(p-1))/p^2}$. Therefore

$$|a_k(x^{k-1} + x^{k-2}y + \cdots + y^{k-1})|_p < |a_k|_p \left(\frac{1}{p}\right)^{(k-1)(2+1/(p-1))/p^2}, \tag{3.12}$$

where the last inequality is strict since $a_k \neq 0$ (from the definition of $E(X)$, its coefficients are all positive). We want to show the last expression is at most 1.

If $2 \leq k < p^2$ the kth coefficients of $E(X)$ and $\mathrm{AH}(X)$ agree, so $a_k \in \mathbf{Z}_p$ and thus

$$|a_k|_p \left(\frac{1}{p}\right)^{(k-1)(2+1/(p-1))/p^2} < |a_k|_p \leq 1.$$

If $k \geq p^2$, put the upper bound on $|a_k|_p$ from Theorem 3.6 into (3.12):

$$\begin{aligned}
|a_k(x^{k-1} + x^{k-2}y + \cdots + y^{k-1})|_p &< |a_k|_p \left(\frac{1}{p}\right)^{(k-1)(2+1/(p-1))/p^2} \\
&\leq p^{(k/p^2)(2+1/(p-1))-1/(p-1)} \left(\frac{1}{p}\right)^{(k-1)(2+1/(p-1))/p^2} \\
&= p^{(2+1/(p-1))/p^2-1/(p-1)} \\
&= p^{-(p-1)/p^2} \\
&< 1.
\end{aligned}$$

□

It is critical for this proof that we used $s_p(i)/(p-1)$ in the proof of Theorem 3.6, since that is how we got the term $-1/(p-1)$ in the exponent of the upper bound on $|a_k|_p$. Without that term, the upper bound at the end of the proof of Theorem 3.7 would have been $p^{(2+1/(p-1))/p^2}$, which is greater than 1 instead of less than 1.

Corollary 3.8. *For $x \in D_2$, $E(x) = e^{x+x^p/p}$ if and only if $x \in D$.*

Proof. We proved the "if" direction in Theorem 3.3. Conversely, if $x \in D_2$ and $E(x) = e^y$ for a $y \in D$ then $|E(x) - 1|_p < (1/p)^{1/(p-1)}$, so also $|x|_p < (1/p)^{1/(p-1)}$ by Theorem 3.7. □

Corollary 3.9. *If x is a nonzero root of $X + X^p/p$ then $E(x)$ is a nontrivial pth root of unity.*

Proof. By Theorem 3.3, $E(x)^p = 1$. We show $E(x) \neq 1$ in two ways.

Method 1: Since $E(X)$ is an isometry on D_2, $E(x) = 1$ only for $x = 0$.

Method 2: Since $E(X)$ is an isometry, $|E(x) - 1|_p = |x|_p = (1/p)^{1/(p-1)}$, so $E(x) \neq 1$. □

The nonzero roots of $X + X^p/p$ are roots of $X^{p-1} + p$. Letting π be a p-adic root of $X^{p-1} + p$, so $\pi^{p-1} = -p$ and $|\pi|_p = (1/p)^{1/(p-1)}$. Theorem 3.2 says the disc of convergence of $E(X)$ is the x with $|x|_p < (1/p)^{(2+1/(p-1))/p^2}$, so the disc of convergence of $E(\pi X)$ is the x with $|\pi x|_p < (1/p)^{(2+1/(p-1))/p^2}$, which is equivalent to $|x|_p < (1/p)^{(2+1/(p-1))/p^2 - 1/(p-1)} = p^{(p-1)/p^2}$. The nonzero roots of $X + X^p/p$ are $\zeta\pi$ where $\zeta^{p-1} = 1$, and by Corollary 3.9, $E(\pi X)$ is a nontrivial p-th root of unity when we substitute for X the different $(p-1)$-th roots of unity.

Theorem 3.10. *Writing $E(\pi X) = \sum_{k\geq 0} b_k X^k$, we have $\operatorname{ord}_p(b_k) \geq \frac{p-1}{p^2}k + \frac{1}{p-1}$ if $k \geq (p+1)/2$ and not if $k < (p+1)/2$.*

Proof. Letting $E(X) = \sum_{k\geq 0} a_k X^k$ as before, $E(\pi X) = \sum_{k\geq 0} a_k \pi^k X^k$, so $b_k = a_k \pi^k$. For $k \geq (p+1)/2$, the upper bound on $|a_k|_p$ in Theorem 3.6 is equivalent to the lower bound $\operatorname{ord}_p(a_k) \geq -(k/p^2)(2 + 1/(p-1)) + 1/(p-1)$, and in this case

$$\begin{aligned}
\operatorname{ord}_p(b_k) &= \operatorname{ord}_p(a_k) + \frac{k}{p-1} \\
&\geq -\frac{k}{p^2}\left(2 + \frac{1}{p-1}\right) + \frac{1}{p-1} + \frac{k}{p-1} \\
&= -\frac{2p-1}{p^2(p-1)}k + \frac{1}{p-1} + \frac{k}{p-1} \\
&= \left(\frac{1}{p-1} - \frac{2p-1}{p^2(p-1)}\right)k + \frac{1}{p-1} \\
&= \frac{p-1}{p^2}k + \frac{1}{p-1}.
\end{aligned}$$

If $k < (p+1)/2$ then $k < p$, so $b_k = a_k\pi^k = \pi^k/k!$ and $\operatorname{ord}_p(b_k) = \operatorname{ord}_p(\pi^k) = k/(p-1)$. Therefore we want to show $\frac{k}{p-1} < \frac{p-1}{p^2}k + \frac{1}{p-1}$, which is equivalent to $k < p^2/(2p-1)$. Does $k < (p+1)/2 \Rightarrow k < p^2/(2p-1)$? Not if $k \in \mathbf{R}$, since $p^2/(2p-1) < (p+1)/2$, but we are okay for $k \in \mathbf{Z}$: when $p = 2$ we want $k < 3/2 \Rightarrow k < 4/3$ for $k \in \mathbf{Z}$, which is true, and when p is an odd prime we want $k \leq (p-1)/2 \Rightarrow k < p^2/(2p-1)$ for $k \in \mathbf{Z}$, which is true since $(p-1)/2 < p^2/(2p-1)$. □

4. Getting pth-power roots of unity from $\exp(X + X^p/p + \cdots + X^{p^n}/p^n)$

For $n \geq 0$, define the nth truncated Artin–Hasse series

$$\mathrm{AH}_n(X) = \exp\left(X + \frac{X^p}{p} + \cdots + \frac{X^{p^n}}{p^n}\right) = \exp\left(\sum_{j=0}^{n} \frac{X^{p^j}}{p^j}\right).$$

For example, $\mathrm{AH}_0(X) = e^X$ and $\mathrm{AH}_1(X) = E(X)$.

Our goal is to find the disc of convergence of $\mathrm{AH}_n(X)$ and show that when $n \geq 1$ and x is a root of $X + X^p/p + \cdots + X^{p^n}/p^n$ in that disc, $\mathrm{AH}_n(x)$ is a p^nth root of unity and compute its order. We already did this for $n = 1$ in the previous section, and everything in this section will be a straightforward generalization of the case $n = 1$ except at the end.

Theorem 4.1. *The disc of convergence of* $\mathrm{AH}_n(X)$ *is*

$$D_{n+1} = \{x : |x|_p < (1/p)^{(n+1+1/(p-1))/p^{n+1}}\}.$$

Proof. This is like the proof of Theorem 3.2, using

$$\mathrm{AH}_n(X) = \mathrm{AH}(X) \prod_{j \geq n+1} e^{-X^{p^j}/p^j} = \mathrm{AH}(X) \exp\left(\sum_{j \geq n+1} -\frac{X^{p^j}}{p^j}\right) \tag{4.1}$$

as a generalization of (3.1) and (3.3). We will make a few remarks but leave it to the reader to check the details carry over.

Theorem 2.2 implies the single exponential factor on the right in (4.1) converges on D_{n+1}, as does $\mathrm{AH}(X)$, so $\mathrm{AH}_n(X)$ converges on D_{n+1}. To prove $\mathrm{AH}_n(X)$ does not converge outside of D_{n+1}, rewrite (4.1) as

$$e^{-X^{p^{n+1}}/p^{n+1}} = \mathrm{AH}_n(X)\,\mathrm{AH}(X)^{-1} \exp\left(\sum_{j \geq n+2} X^{p^j}/p^j\right).$$

By another use of Theorem 2.2, the third factor on the right converges on D_{n+2}, as does $\mathrm{AH}(X)^{-1}$, so if $\mathrm{AH}_n(X)$ converges somewhere outside D_{n+1} then so does $e^{-X^{p^{n+1}}/p^{n+1}}$, which is false. □

Theorem 4.2. *If* $x \in D$ *then* $\mathrm{AH}_n(x) = e^{x+x^p/p+\cdots+x^{p^n}/p^n}$. *If* $x \in D_{n+1}$ *then* $\mathrm{AH}_n(x)^{p^n} = e^{p^n(x+x^p/p+\cdots+x^{p^n}/p^n)}$. *In particular, if* $x + x^p/p + \cdots + x^{p^n}/p^n = 0$ *and* $x \in D_{n+1}$ *then* $\mathrm{AH}_n(x)^{p^n} = 1$.

Proof. This is like the proof of Theorem 3.3. By the proof of Theorem 2.4, if $x \in D$ then $|x^{p^j}/p^j|_p < |x|_p$ for $j \geq 1$, so Theorem 2.2 with $f(X) = \exp(X)$ and $g(X) = \sum_{j=0}^{n} X^{p^j}/p^j$ implies the first part of the theorem.

The proof of the second part of the theorem is similar to the proof of the second part of Theorem 3.3. In the power series identity

$$\mathrm{AH}_n(X)^{p^n} = \exp\left(\sum_{j=0}^{n} p^{n-j} X^{p^j}\right)$$

we can use Theorem 2.2 on the right side if all $x \in D_{n+1}$ satisfy $p^{n-j}x^{p^j} \in D$ for $0 \leq j \leq n$. We have

$$|p^{n-j}x^{p^j}|_p < \left(\frac{1}{p}\right)^{(n-j)+p^j(n+1+1/(p-1))/p^{n+1}},$$

so to show $|p^{n-j}x^{p^j}|_p < (1/p)^{1/(p-1)}$ we want to show for $0 \leq j \leq n$ that

$$n - j + \frac{p^j(n+1+1/(p-1))}{p^{n+1}} \geq \frac{1}{p-1}.$$

Clearing denominators, this inequality is the same as

$$p^{n+1}(p-1)(n-j) + (p-1)p^j(n+1) + p^j \geq p^{n+1}.$$

If $j < n$ this inequality is true since the first term on the left is at least p^{n+1} and the other terms are positive. If $j = n$ then the inequality becomes

$$(p-1)p^n(n+1) + p^n \geq p^{n+1}.$$

After dividing by p^n and rearranging terms this is the same as $(p-1)n \geq 0$, which is true.

If $x + x^p/p + \cdots + x^{p^n}/p^n = 0$ and $x \in D_{n+1}$ then $\mathrm{AH}_n(x)^{p^n} = e^{p^n(0)} = 1$. □

A difference between Theorem 4.2 and Theorem 3.3 is that for $n > 1$ some roots of $X + X^p/p + \cdots + X^{p^n}/p^n$ in $\mathbf{C}_p$ may not be in the disc of convergence of $\mathrm{AH}_n(X)$! See Theorem 4.9. This is a contrast to $n = 1$ and $n = \infty$ (that is, $\mathrm{AH}(X)$) and that's why we had to be explicit at the end of Theorem 4.2 that x is in D_{n+1} when $x + x^p/p + \cdots + x^{p^n}/p^n = 0$.

To show $\mathrm{AH}_n(X)$ at roots of $X + X^p/p + \cdots + X^{p^n}/p^n$ in D_{n+1} has a predictable order as a root of unity, we will prove $\mathrm{AH}_n(X)$ is an isometry on its disc of convergence. We start with a generalization of Lemma 3.4.

Lemma 4.3. *Let $u_j \in \mathbf{Z}_p^\times$ for $j \geq n+1$. Writing*

$$\prod_{j \geq n+1} e^{u_j X^{p^j}/p^j} = \sum_{k \geq 0} c_{n,k} X^k,$$

we have $c_{n,k} = 0$ if $p^{n+1} \nmid k$, and if $p^{n+1} \mid k$ then

$$\mathrm{ord}_p(c_{n,k}) = -\frac{k}{p^{n+1}}\left(n + 1 + \frac{1}{p-1}\right) + \frac{s_p(k)}{p-1}.$$

Proof. The proof is similar to that of Lemma 3.4. Details are left to the reader. □

As in Lemma 3.4, the way to think about Lemma 4.3 is that it tells us the p-adic absolute value of $c_{n,k}$ for each k equals the p-adic absolute value of the coefficient of degree k in the first factor of the product.

Theorem 4.4. *Setting $\mathrm{AH}_n(X) = \sum_{k \geq 0} a_{n,k} X^k$, for $k \geq p^{n+1}$ we have the bound*

$$|a_{n,k}|_p \leq p^{(k/p^{n+1})(n+1+1/(p-1))-1/(p-1)}.$$

Proof. This is similar to the proof of Theorem 3.6 for $k \geq p^2$, where $a_{1,k}$ here is a_k there. □

Remark 4.5. For $k \geq p^{n+1}$ the upper bound on $|a_{n,k}|_p$ is equivalent to the lower bound

$$\mathrm{ord}_p(a_{n,k}) \geq -\frac{k}{p^{n+1}}\left(n + 1 + \frac{1}{p-1}\right) + \frac{1}{p-1},$$

which can be weakened to

$$\mathrm{ord}_p(a_{n,k}) \geq -\frac{k}{p^{n+1}}\left(\frac{1}{p-1} + n + 1\right),$$

and this is valid for all $k \geq 0$. (For $0 \leq k < p^{n+1}$ the coefficients of $\mathrm{AH}_n(X)$ and $\mathrm{AH}(X)$ are equal and thus lie in $\mathbf{Z}_p$.) This weaker bound goes back to Dwork's work on the Weil conjectures [1, pp. 55–56], where it appears in a more cryptic form as [1, Equation 4.7]. The additional term $1/(p-1)$ in our lower bound on $\mathrm{ord}_p(a_{n,k})$ for $k \geq p^{n+1}$ will be useful, as it was in the previous section when $n = 1$.

Theorem 4.6. *For all x and y in D_{n+1}, $|\mathrm{AH}_n(x) - \mathrm{AH}_n(y)|_p = |x - y|_p$.*

Proof. The case $n = 1$ is Theorem 3.7, whose proof will carry over. Since $a_{n,0} = a_{n,1} = 1$,

$$\mathrm{AH}_n(x) - \mathrm{AH}_n(y) = x - y + \sum_{k \geq 2} a_{n,k}(x^k - y^k),$$

so as in the proof of Theorem 3.7 it suffices to show for $x \neq y$ and $k \geq 2$ that

$$|a_{n,k}(x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1})|_p < 1. \tag{4.2}$$

This holds for $2 \leq k < p^{n+1}$ since $a_{n,k} \in \mathbf{Z}_p$ and x and y have absolute value less than 1.

For $k \geq p^{n+1}$ we have an upper bound on $|a_{n,k}|_p$ from Theorem 4.4. Since x and y are in D_{n+1}, the left side of (4.2) is less than

$$p^{(k/p^{n+1})(n+1+1/(p-1))-1/(p-1)}\left(\frac{1}{p}\right)^{(k-1)(n+1+1/(p-1))/p^{n+1}} = p^{(n+1+1/(p-1))/p^{n+1}-1/(p-1)}.$$

The exponent of p here is

$$\frac{n+1+1/(p-1)}{p^{n+1}} - \frac{1}{p-1} = \frac{(p-1)(n+1)+1-p^{n+1}}{p^{n+1}(p-1)} = -\frac{1}{p^{n+1}}\left(\frac{p^{n+1}-1}{p-1} - (n+1)\right),$$

which is negative, and that proves (4.2). □

Corollary 4.7. *For $x \in D_{n+1}$,*

$$\mathrm{AH}_n(x) = e^{x+x^p/p+\cdots+x^{p^n}/p^n}$$

if and only if $x \in D$.

Proof. The “if” direction is in Theorem 4.2. The “only if” direction follows from Theorem 4.6 in the same way Corollary 3.8 follows from Theorem 3.7. □

The roots of $X + X^p/p + X^{p^2}/p^2 + \cdots + X^{p^n}/p^n$ in $\mathbf{C}_p$ can be described using Newton polygons and derivatives: besides the root 0, for $1 \leq j \leq n$ there are $p^j - p^{j-1} = \varphi(p^j)$ simple roots with valuation $1/\varphi(p^j)$.

Corollary 4.8. *If x is a root of $X + X^p/p + \cdots + X^{p^n}/p^n$ in D_{n+1} with $\mathrm{ord}_p(x) = 1/\varphi(p^j)$ then $\mathrm{AH}_n(x)$ is a root of unity of order p^j.*

Proof. By Theorem 4.2, $\mathrm{AH}_n(x)^{p^n} = 1$. The order of $\mathrm{AH}_n(x)$ is p^j since $|\mathrm{AH}_n(x) - 1|_p = |x|_p = (1/p)^{1/(p^{j-1}(p-1))}$. □

We end with a theorem that tell us which roots of $X + X^p/p + \cdots + X^{p^n}/p^n$ are in D_{n+1}.

Theorem 4.9. *If x is a nonzero root of $X + X^p/p + \cdots + X^{p^n}/p^n$ and $\mathrm{ord}_p(x) = 1/\varphi(p^j)$, where $1 \leq j \leq n$, then $x \in D_{n+1}$ if and only if*

$$1 + p + p^2 + \cdots + p^{n+1-j} > n+1.$$

In particular, roots with valuation $1/\varphi(p^j)$ are in D_{n+1} if n is sufficiently large compared to j.

Proof. We want to know when $\mathrm{ord}_p(x) = 1/\varphi(p^j) \Longrightarrow \mathrm{ord}_p(x) > (n+1+1/(p-1))/p^{n+1}$:

$$\begin{aligned}\frac{1}{p^{j-1}(p-1)} > \frac{n+1+1/(p-1)}{p^{n+1}} &\iff p^{n+2-j} > (p-1)(n+1)+1\\ &\iff \frac{p^{n+2-j}-1}{p-1} > n+1\\ &\iff 1+p+p^2+\cdots+p^{n+1-j} > n+1.\end{aligned}$$

If p and j are fixed, this inequality holds for sufficiently large $n > j$. The inequality holds if $j = 1$ for all p and all $n \geq 1$. It also holds for all $j \leq n$ if $p > n$. But if $j = n$ and $p \leq n$ then the inequality fails. □

Example 4.10. If $n = 3$ and $p = 2$ or 3 then $j = 1$ or 2 work but $j = 3$ does not. If $n = 9$ and $p = 2$ then $j = 1, \ldots, 7$ work but $j = 8$ or 9 do not.

5. Distribution of coefficients of $\mathrm{AH}(X)$ in $\mathbf{Z}_p$

Write $\mathrm{AH}(X)$ as $\mathrm{AH}_p(X)$ to indicate its dependence on p.[3] The coefficients of $\mathrm{AH}_p(X)$ are a sequence of p-adic integers with no simple formula. Do they behave like a random sequence?

In Table 1 we provide the natural density of the coefficients up to some degree having a particular ord_p value of v. Decimals are truncated at the fifth digit, so the final digits in the table are correct. For example, among the first 1500 coefficients of $\mathrm{AH}_2(X)$, about .24666 of them have ord_2 value 1. (The number of rows for each prime is chosen so every possible coefficient valuation that arises is accounted for in one of the densities.) The last column gives the Haar measure of the set of p-adic integers with ord_p value v. The table should be read row by row, from left to right, with the final entry in each row being a conjectured limiting value. Another way to read the table is column by column, from top to bottom for each prime, and check that division of an entry by p is approximately equal to the number below it.

Calculations of coefficients of $\mathrm{AH}_p(X)$ for this table were initially made with the exponential formula for the series, but the alternate formula

$$\mathrm{AH}_p(X) = \prod_{\substack{k\geq 1\\ p\nmid k}}(1-X^k)^{-\mu(k)/k}$$

from the proof of Theorem 2.1 is more convenient for large-scale computations: it has the p-adic integrality of the coefficients built into it.

In Table 2 we give the exact number of coefficients up to a given bound with a given ord_p value. For example, 190 of the first 400 coefficients of $\mathrm{AH}_2(X)$ have ord_2 value 0.

These tables of ord_p values are a concise way to present evidence for uniform distribution, although they only reflect a coarser type of distribution in $\mathbf{Z}_p$, relative to the balls containing 0 rather than all balls in $\mathbf{Z}_p$. We provide in Table 3 the total number of coefficients of $\mathrm{AH}_3(X)$, among the first 6000, falling into a given congruence class of $\mathbf{Z}_3$ modulo 3^n for $n = 1, 2, 3$. If the coefficients are uniformly distributed, the number of coefficients in each congruence class modulo 3, 9, and 27 should be, respectively, around 2000, 667, and 222.

Table 4 gives the number (and relative proportion) of coefficients of $\mathrm{AH}_3(X)$ among the first 10000 with a particular ord_3 value, counting initial segments of length 4000, 5000, ..., 10000. For example, 2618 of the first 4000 coefficients of $\mathrm{AH}_3(X)$ are 3-adic units. No coefficient among the first 10000 is divisible by 3^8.

Based on the available data, the following conjecture seems reasonable.

Conjecture 5.1. *The coefficients of* $\mathrm{AH}_p(X)$ *are uniformly distributed in* $\mathbf{Z}_p$ *with respect to Haar measure.*

In particular, for each $v \geq 0$ there should be infinitely many coefficients of $\mathrm{AH}_p(X)$ with ord_p value v, but this remains an open problem except in the case $v = 0$, since the proof of Theorem 2.10 shows $\mathrm{AH}_p(X)$ has infinitely many coefficients in $\mathbf{Z}_p^\times$.

[3] There should be no confusion with the previous notation $\mathrm{AH}_n(X)$ for truncated Artin–Hasse series.

TABLE 1. Densities of coefficients of $\mathrm{AH}_p(X)$, by ord_p value

p	v	#/400	#/500	#/800	#/1000	#/1500	#/2000	#/3000	$(p-1)/p^{v+1}$
2	0	.47500	.48600	.49750	.50400	.50000	.49350	.49833	.50000
	1	.25000	.24200	.25125	.24700	.24666	.24500	.25033	.25000
	2	.15000	.14000	.12875	.12600	.12933	.13300	.12900	.12500
	3	.06250	.06200	.06000	.05500	.06133	.06250	.06066	.06250
	4	.03250	.03600	.02875	.03400	.03133	.03300	.03000	.03125
	5	.00750	.01200	.01000	.01100	.01066	.01450	.01466	.01562
	6	.00750	.00800	.01125	.00900	.00933	.00850	.00700	.00781
	7	.00500	.00400	.00500	.00600	.00533	.00450	.00400	.00390
	8	.00500	.00600	.00500	.00500	.00333	.00350	.00400	.00195
	9	.00500	.00400	.00250	.00300	.00200	.00150	.00100	.00097
	10	.00000	.00000	.00000	.00000	.00066	.00050	.00033	.00048
	11	.00000	.00000	.00000	.00000	.00000	.00000	.00033	.00024
	12	.00000	.00000	.00000	.00000	.00000	.00000	.00033	.00012
3	0	.64000	.65800	.65125	.65600	.65800	.65500	.65400	.66666
	1	.27500	.26400	.24625	.23500	.22866	.23700	.23366	.22222
	2	.05250	.04600	.06875	.07800	.08000	.07400	.07866	.07407
	3	.02000	.02000	.02125	.01900	.02200	.02200	.02266	.02469
	4	.00750	.00800	.00875	.00900	.00866	.00950	.00733	.00823
	5	.00500	.00400	.00375	.00300	.00266	.00200	.00266	.00274
	6	.00000	.00000	.00000	.00000	.00000	.00000	.00066	.00091
	7	.00000	.00000	.00000	.00000	.00000	.00050	.00033	.00030
5	0	.81500	.82200	.81375	.81600	.80000	.79600	.79333	.80000
	1	.14000	.14000	.15000	.14800	.15733	.16100	.16200	.16000
	2	.03500	.03000	.02875	.02900	.03400	.03500	.03633	.03200
	3	.00750	.00600	.00625	.00600	.00800	.00650	.00700	.00640
	4	.00250	.00200	.00125	.00100	.00066	.00100	.00066	.00128
	5	.00000	.00000	.00000	.00000	.00000	.00050	.00066	.00025
7	0	.84750	.85600	.84875	.84600	.84666	.84800	.84966	.85714
	1	.12750	.11600	.12000	.12400	.12266	.12450	.12433	.12244
	2	.01750	.02200	.02750	.02700	.02733	.02350	.02300	.01749
	3	.00500	.00400	.00250	.00200	.00266	.00300	.00233	.00249
	4	.00250	.00200	.00125	.00100	.00066	.00050	.00033	.00035
	5	.00000	.00000	.00000	.00000	.00000	.00000	.00033	.00005

Table 2. Number of coefficients of $\mathrm{AH}_p(X)$, by ord_p value

p	v	# ≤ 400	# ≤ 500	# ≤ 800	# ≤ 1000	# ≤ 1500	# ≤ 2000	# ≤ 3000
2	0	190	243	398	504	750	987	1495
	1	100	121	201	247	370	490	751
	2	60	70	103	126	194	266	387
	3	25	31	48	55	92	125	182
	4	13	18	23	34	47	66	90
	5	3	6	8	11	16	29	44
	6	3	4	9	9	14	17	21
	7	2	2	4	6	8	9	12
	8	2	3	4	5	5	7	12
	9	2	2	2	3	3	3	3
	10	0	0	0	0	1	1	1
	11	0	0	0	0	0	0	1
	12	0	0	0	0	0	0	1
3	0	256	329	521	656	987	1310	1962
	1	110	132	197	235	343	474	701
	2	21	23	55	78	120	148	236
	3	8	10	17	19	33	44	68
	4	3	4	7	9	13	19	22
	5	2	2	3	3	4	4	8
	6	0	0	0	0	0	0	2
	7	0	0	0	0	0	1	1
5	0	326	411	651	816	1200	1592	2380
	1	56	70	120	148	236	322	486
	2	14	15	23	29	51	70	109
	3	3	3	5	6	12	13	21
	4	1	1	1	1	1	2	2
	5	0	0	0	0	0	1	2
7	0	339	428	679	846	1270	1696	2549
	1	51	58	96	124	184	249	373
	2	7	11	22	27	41	47	69
	3	2	2	2	2	4	6	7
	4	1	1	1	1	1	1	1
	5	0	0	0	0	0	0	1

Table 3. Data for first 6000 coefficients of $\mathrm{AH}_3(X)$

n	0	1	2
$\# \equiv n \bmod 3$	2053	1980	1967

n	0	1	2	3	4	5	6	7	8
$\# \equiv n \bmod 9$	671	641	640	715	681	660	667	658	667

n	0	1	2	3	4	5	6	7	8
$\# \equiv n \bmod 27$	206	218	192	237	250	221	220	235	236
n	9	10	11	12	13	14	15	16	17
$\# \equiv n \bmod 27$	234	214	228	233	209	212	212	216	222
n	18	19	20	21	22	23	24	25	26
$\# \equiv n \bmod 27$	231	209	220	245	222	227	235	207	209

Table 4. Data for First 10000 Coefficients of $\mathrm{AH}_3(X)$

v	0	1	2	3	4	5	6	7
$\# \leq 4000$	2618	937	304	97	29	11	3	1
$\#/4000$	.65450	.23425	.07600	.02425	.00725	.00275	.00075	.00025
$\# \leq 5000$	3276	1173	380	119	35	13	3	1
$\#/5000$	.65520	.23460	.07600	.02380	.00700	.00260	.00060	.00020
$\# \leq 6000$	3947	1382	465	141	44	16	3	2
$\#/6000$	.65783	.23033	.07750	.02350	.00733	.00266	.00050	.00033
$\# \leq 7000$	4627	1581	553	160	53	21	3	2
$\#/7000$	.66100	.22585	.07900	.02285	.00757	.00300	.00042	.00028
$\# \leq 8000$	5270	1811	635	189	65	23	4	3
$\#/8000$	.65875	.22637	.07937	.02362	.00812	.00287	.00050	.00037
$\# \leq 9000$	5921	2046	696	221	81	28	4	3
$\#/9000$	.65788	.22733	.07733	.02455	.00900	.00311	.00044	.00033
$\# \leq 10000$	6578	2283	770	243	87	29	5	5
$\#/10000$	.65780	.22830	.07700	.02430	.00870	.00290	.00050	.00050

References

[1] B. Dwork, "On the zeta function of a hypersurface," *Publ. Math. IHES* **12** (1962), 5–68.

[2] F. Gouvêa, "*p*-adic Numbers: An Introduction," 2nd ed., Springer-Verlag, New York, 1997.

[3] S. Lang, "Cyclotomic Fields I and II," Springer-Verlag, New York, 1990.

[4] A. M. Robert, "A Course in *p*-Adic Analysis," Springer-Verlag, New York, 2000.

[5] W. H. Schikhof, "Ultrametric Calculus: An Introduction to *p*-Adic Analysis," Cambridge Univ. Press, Cambridge, 1984.